DEPARTMENT OF THE ARMY
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
JOINT FORCE HEADQUARTERS-NATIONAL CAPITAL REGION
102 3RD AVENUE, BLDG 39, SUITE 2
FORT LESLEY J. MCNAIR, DC 20319-5031

ANPM

MAR 14 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter – Operations Security (OPSEC) – Memorandum #24

1. REFERENCES.

a. Directive 5205.02E, Department of Defense, subject: DoD Operations Security (OPSEC) Program.

b. Army Regulation 530-1 (Operations Security (OPSEC)).

c. Army Regulation 360-1 (Army Public Affairs Program).

d. Army Regulation 25-2 (Information Assurance).

2. PURPOSE. This memorandum establishes OPSEC policy for Joint Force Headquarters-National Capital Region/U.S. Army Military District of Washington (JFHQ-NCR/USAMDW) based on DoD and Army OPSEC regulations.

3. APPLICABILITY. This policy applies to ALL military personnel, civilian employees, and contract personnel assigned or attached to Headquarters, JFHQ-NCR and USAMDW, as well as USAMDW subordinate commands, elements, and other activities. Senior Command installations will incorporate this policy letter into their OPSEC programs to support USAMDW force protection responsibilities. Support units and service components of JFHQ-NCR are encouraged to adopt this policy into their own command policies. This policy letter supersedes all previous editions.

4. POLICY. Operations Security is everyone's responsibility. OPSEC is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. It is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities. Operations Security is a Commander's Program, and while it is primarily an operations function, robust OPSEC practices and procedures must be integrated into all day-to-day activities by the entire workforce. The OPSEC Program Manager is the focal point for coordinating the implementation of the OPSEC program with designated OPSEC

Officers and Coordinators through the Headquarters and at USAMDW installation and subordinate levels.

5. PROCEDURES.

a. OPSEC requirements for JFHQ-NCR/USAMDW operational planning and execution.

(1) All JFHQ-NCR/USAMDW Headquarters staff elements or directorates responsible for planning missions, activities, or events will designate an OPSEC Coordinator to assist the OPSEC Program Manager with incorporating the OPSEC process into planning and coordination phases of operations. The OPSEC Coordinators will include an OPSEC Annex or Appendix into respective plans and orders with the assistance of the OPSEC Program Manager.

(2) Subordinate commands, elements, and activities will incorporate the OPSEC process into plans and orders. When officially tasked in JFHQ-NCR/USAMDW plans or orders, senior command installations and supporting service components will comply with OPSEC provisions.

(3) The JFHQ-NCR/USAMDW Critical Information List (CIL) is attached as an enclosure.

b. OPSEC requirements for JFHQ-NCR/USAMDW personnel and day-to-day operations.

(1) Official work products (e.g., presentations not intended for the public, email printouts, electronic and recordable storage media, office correspondence, hand notes, any form of personal information, training schedules or calendars, or working papers) containing critical information **will not** be discarded as regular refuse or paper recycling. Any document containing operational or mission critical information not otherwise classified, will be marked as FOUO.

(2) Individuals will destroy these types of documents or information in a manner that defeats reconstruction by using a high-security or standard office shredder, tearing into small pieces, or utilizing the command's burn-bag program. Contact the Command Security Manager or OPSEC Program Manager for guidance on what types of documents should be destroyed.

(3) If Secure Telephone Equipment (STE) is available, operationally critical information should be communicated through secure means. When an encryption feature is available on unclassified networks, encrypt e-mail messages containing critical or FOUO information.

(4) All JFHQ-NCR/USAMDW personnel will maintain annual OPSEC certification. In addition, all JFHQ-NCR/USAMDW personnel will consult with their immediate supervisor, OPSEC Officer, or Public Affairs Office (PAO) for an OPSEC review prior to publishing or posting official information in public forums (including newspapers, journals, bulletin boards, the internet, such as email, web-based chat-rooms, logs or "blogs," social websites, or other

forms of dissemination or documentation). Additionally, any office providing information to the PAO for public release will ensure an OPSEC review is conducted (AR 360–1, Paragraph 5-4).

(5) Prior to responding to Freedom of Information Act (FOIA) requests, an OPSEC review will be accomplished to ensure indicators of critical information are not released.

c. OPSEC coordination with other security programs.

(1) Coordination between OPSEC and traditional security programs helps ensure the protection of unclassified critical information, and classified national security information.

(2) OPSEC and Information Assurance (IA) work together to protect information through policies that achieve acceptable levels of IA in the engineering, implementation, operation, and maintenance of information systems. Official DoD telecommunication systems, including telephones and computer networks, are subject to monitoring at all times for security purposes. All users will immediately report network or cyber security incidents to the Information Assurance Program Manager.

d. Personnel will report any suspected OPSEC incident or violation to their organization OPSEC Officer or security manager for follow-up investigation. Other suspicious elicitation attempts should be reported to the 902d MI Group at (703) 805-3008, or the 1-(800) CALL-SPY hotline, leaving a message with name and telephone number, and no further details.

6. The point of contact for this policy is the JFHQ-NCR/USAMDW OPSEC Program Manager at (202) 685-2901.

Encl
Critical Information List (CIL)

BRADLEY A. BECKER
Major General, US Army
Commanding

DISTRIBUTION:
A

JFHQ-NCR/USAMDW CRITICAL INFORMATION LIST (CIL)

1. (U//FOUO) The Critical Information List (CIL) includes specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment. Critical information is susceptible to collection by adversaries through indicators (friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information), and vulnerabilities (conditions in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making).

2. (U//FOUO) The JFHQ-NCR/USAMDW Critical Information List (CIL) is:

a. (U//FOUO) Information pertaining to access control, physical security, and protection of installations and critical assets (e.g., personnel, facilities, equipment, or information) (OPR: PM/PD).

b. (U//FOUO) Current and projected operational status (including capabilities and readiness) of assigned forces and command and control (C2) systems (OPR: J3, OCR: J6).

c. (U//FOUO) Information regarding deployment/redeployment of JFHQ-NCR personnel and assets to support real-world missions (i.e. overseas contingency operations) (OPR: J3).

d. (U//FOUO) Location/disposition of forces during events or incident response, including all DoD and interagency response forces (OPR: J36, OCR: J35).

e. (U//FOUO) Posture or preparation of Base Support Installations (BSI) in support of Joint Reception, Staging, Onward Movement & Integration (JRSOI) operations (OPR: J3, OCR: J1/J4).

f. (U//FOUO) Operational requirements, capabilities, or shortfalls pertaining to preparation and execution of JFHQ-NCR COOP/COG operations (OPR: J3, OCR: PM/PD).

Enclosure